REMARKS

The Examiner has rejected Claims 1-3, 5-9, 11-12, 14-19, 21-25, 27-28, 30-35, 37-41, 43-44, 46-51, 53-57, 59-60, 62-67, 69-73, 75-76, 78-83, 85-89, 91-92, and 94-96 under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. In response, applicant asserts that the Examiner's rejections are avoided by virtue of the amendments made to the independent claims.

The Examiner has further rejected Claims 1-3, 5-9, 11-12, 14-19, 21-25, 27-28, and 30-32 under 35 U.S.C. 101 as being directed toward non-statutory subject matter. Applicant has clarified Claim 1 et al. to include a computer program product "embodied on a tangible computer readable medium" in order to avoid such rejection.

The Examiner has still yet further rejected Claims 1-3, 5, 9, 11-12, 14, 17-19, 21, 25, 27-28, 30, 33-35, 37, 41, 43-44, 46, 49-51, 53, 57, 59-60, 62, 65-67, 69, 73, 75-76, 78, 81-83, 85, 89, 91-92, and 94 under 35 U.S.C. 103(a) as being unpatentable over Cozza (U.S. Patent No. 5,649,095) in view of Hypponen et al. (U.S. Patent No. 6,577,920). Applicant respectfully disagrees with such rejection, especially in view of the amendments made hereinabove to the independent claims. Specifically, applicant has amended the independent claims to at least substantially include the subject matter of former dependent Claim 11 et al.

With respect to the independent claims, the Examiner has relied on the following excerpts from the Cozza and Hypponen references to make a prior art showing of applicant's claimed technique "wherein said fingerprint data includes a number of program resource items specified within said resource data" (see this or similar, but not necessarily identical language in the independent claims).

"According to a second aspect of the present invention there is provided a method of screening a software file for viral infection, the method comprising:
defining a first database of known macro virus signatures, a second database of known and certified commercial macro signatures, and a third database of known and certified local macro signatures;
scanning said file to determine whether or not the file contains a macro; and, if the file contains a macro determining a signature for the macro and screening that signature against the signatures contained in said databases; and" (Hypponen, Col. 3, lines 14-25)

"A third example involves the nature of multi-fork file storage on computers such as the Apple Macintosh. **Typically one fork of a file, for example the resource fork on Macintosh computers, may contain a kind of small database which is used to contain many kinds of data, including application code, icons, preferences, strings, templates, and other such items.** A change in size to such a fork may not indicate a change to application code, but rather a change to something else such as user preferences. It is therefore necessary to handle this complexity in a proper manner so as to optimize speed enhancement without compromising scan effectiveness." (Cozza, Col. 2, paragraph 7)

Applicant asserts that the excerpt from Hypponen relied upon by the Examiner discloses "scanning said file to determine whether or not the file contains a macro" and "determining a signature for the macro." In addition, the excerpt from Cozza discloses that "one fork of a file ... may contain a kind of small database which is used to contain many kinds of data, including application code, icons, preferences, strings, templates, and other such items." However, scanning a file and determining the signature of a macro, coupled with a disclosure that a file may contain many kinds of data, simply fails to suggest a technique "wherein said fingerprint data includes a number of program resource items specified within said resource data" (emphasis added), as claimed by applicant.

In addition, the Examiner argued that "Hypponen taught that file signatures should be used to detect viruses (see Hypponen Col. 3 Lines 14-25) and Cozza disclosed the files containing resource items (i.e. application code, icons, preferences, strings, templates) specified within resource data (i.e. resource fork) (See Cozza Col. 2 Paragraph 7)." Applicant respectfully asserts that Hypponen specifically discloses "determining a signature for the **macro** and screening that signature against the signatures contained in said databases" (emphasis added). Additionally, Cozza specifically discloses that the

"resource fork ... may contain a kind of small database which is used to contain many kinds of data, including application code, icons, preferences, strings, templates, and other such items." Clearly, determining a macro signature in a file, combined with the disclosure of a resource fork containing many kinds of data, fails to even suggest a technique "wherein said fingerprint data includes a number of program resource items specified within said resource data" (emphasis added), as claimed by applicant.

Further, with respect to the independent claims, the Examiner has relied on Col. 3 from Cozza and Col. 3, lines 14-25 from Hypponen to make a prior art showing of applicant's claimed technique "wherein said fingerprint data includes a flag indicating which data is included within said fingerprint data" (see this or similar, but not necessarily identical language in the independent claims).

Applicant asserts that the excerpt from Cozza merely discloses two sets of flags, where the first "set of flags the system utilizes a bit field large enough so that there is one bit corresponding to every known Macintosh virus" (Cozza, Col. 5, lines 29-32) and where the "second set of flags resides in the cache information" (Cozza, Col. 5, line 40). The second set is used to indicate "that no virus was found previously in the last scan of the file" or "which virus was found first in the file." (Cozza, Col. 5, lines 42-47). Applicant respectfully asserts that Hypponen teaches "determining a signature for the macro and screening that signature against the signatures contained in said databases" (emphasis added).

However, Cozza's disclosure on flags corresponding to every known virus and flags in the cache indicating previous scan results, when taken in combination with Hypponen's disclosure on determining macro signatures and checking them against signatures in a database, simply fails to suggest a technique "wherein said fingerprint data includes a flag indicating which data is included within said fingerprint data" (emphasis added), as claimed by applicant. There simply is no disclosure in the excerpts from Cozza or Hypponen of "fingerprint data [that] includes a flag," as claimed by applicant.

In addition, the Examiner argued that "Column 3 of Cozza clearly indicated that a set of flags was used to indicate the result (which viruses were found in the file) of the scan." Further, the Examiner argued that "[i]n combination, the signature of the file is used to represent the file during comparison" and "[t]herefore, it is clear that in combination the flags represent which viruses were identified in the signature." However, applicant respectfully asserts that the disclosure of flags representing which viruses were identified in the signature fails to even suggest a technique "wherein said fingerprint data includes a flag indicating which data is included within said fingerprint data" (emphasis added), as claimed by applicant.

To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art and not based on applicant's disclosure. *In re Vaeck*, 947 F.2d 488, 20 USPQ2d 1438 (Fed.Cir.1991).

Applicant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art references, when combined, fail to teach or suggest all of the claim limitations, as noted above. Nevertheless, despite such paramount deficiencies and in the spirit of expediting the prosecution of the present application, applicant has incorporated the subject matter of former Claim 11 et al. into the independent claims.

With respect to the subject matter of former Claim 11 et al (now at least substantially incorporated into the independent claims), the Examiner has relied on the following excerpt from the Cozza reference to make a prior art showing of applicant's

claimed technique "wherein said fingerprint data includes a location within said resource data of an entry specifying a program resource item having a largest size."

> "...size when infecting. If a file's cache information is not marked as having been previously infected by some virus which changes a file's resource fork size, then the file's current resource fork size is compared with the resource fork size stored in the file's cache information in step 66 to see if they are within some predetermined tolerance. The tolerance in this step is determined based upon the size of viruses infecting a file's resource fork on the Apple Macintosh computer, upon the type of file being infected, and upon the typical size changes that might occur in Macintosh applications and other executable files due to minor changes by which the file might modify itself. This tolerance may vary from one file to another depending on file type and other factors. If these sizes are not within the predetermined tolerance, then flags are set for all viruses that might cause this file's resource fork to change size when infecting it in step 68. " (Cozza, Col. 6, lines 29-45 - emphasis added)

Applicant asserts that the excerpt from Cozza relied upon by the Examiner merely discloses comparing "the file's current resource fork size ... with the resource fork size stored in the file's cache information in step 66 to see if they are within some predetermined tolerance" (emphasis added). Clearly, checking a current or stored resource fork size simply fails to even suggest a technique "wherein said fingerprint data includes a location within said resource data of an entry specifying a program resource item having a largest size" (emphasis added), as claimed by applicant. The excerpt from Cozza simply fails to disclose "a program resource item having a largest size," as claimed by applicant.

Applicant further notes that the prior art is also deficient with respect to the dependent claims. For example, with respect to Claim 3 et al., the Examiner has relied on the following excerpt from the Cozza reference to make a prior art showing of applicant's claimed technique "wherein said resource data comparing logic is operable to compare said resource data with characteristics of a plurality of known computer programs to detect if said packed computer program contains one of said plurality of known computer

programs" (see this or similar, but not necessarily identical language in the independent claims).

> "...resource map, and the size of the viruses that can infect a Macintosh resource fork. If it is then necessary to scan the resource fork for resource fork viruses, this is done in step 90. However, scanning is only required those viruses which infect resource forks and for which flags have been set in the steps above." (Cozza, Col. 7, lines 35-40 - emphasis added)

Applicant asserts that the excerpt from Cozza relied upon by the Examiner merely teaches that "[i]f it is then necessary to scan the resource fork for resource fork viruses," then "scanning is only required those viruses which infect resource forks and for which flags have been set." However, Cozza's disclosure to scan the resource fork for only those viruses which infect resource forks fails to even suggest a technique "wherein said resource data comparing logic is operable to compare said **resource data** with characteristics of a plurality of known computer programs to detect if said packed computer program contains one of said plurality of known computer programs" (emphasis added), as claimed by applicant.

Further, with respect to Claim 9 et al., the Examiner has relied on the following excerpts from the Hypponen and Cozza references to make a prior art showing of applicant's claimed technique "wherein said fingerprint data includes a checksum value calculated in dependence upon one or more of: a number of program resource items specified beneath each node within hierarchically arranged resource data; string names associated with program resource items within said resource data; and sizes of program resource items within said resource data."

> '..."signatures" previously determined for respective macros. For the purposes of this example, the signature used is a checksum derived using a suitable checksum calculation algorithm, such as the US Department of Defence Secure Hash Algorithm (SHA) or the older CRC 32 algorithm.' (Hypponen, Col. 4, lines 55-59 - emphasis added)

> "...is not a copy, and that the volume has not been reformatted; and 4) checksum to verify the file's contents. One suitable

> checksum could be determined by starting with an arbitrary (randomly selected) string of 4 hexadecimal bytes, called the key, which is known to the scanning program. **An EOR (i.e., Exclusive Or) operation is performed on each long word (4 bytes) of the cache to the key.** The result is the checksum. Simple variations of this may be used if the cache information is not a multiple of 4 bytes long." (Cozza, Col. 5, lines 1-9 - emphasis added)

Applicant asserts that the excerpt from Hypponen relied upon by the Examiner merely discloses that "the signature used is a checksum derived using a suitable checksum calculation algorithm." Additionally, applicant asserts that Cozza discloses using a "checksum to verify the [scan information cache] file's contents" which is accomplished by "[a]n EOR ... operation [which] is performed on each long word (4 bytes) of the cache to the key." However, obtaining the checksum of the scan information cache file simply fails to meet a technique "wherein said fingerprint data includes a checksum value calculated in dependence upon one or more of: a number of program resource items specified beneath each node **within hierarchically arranged resource data**; string names associated with program resource items **within said resource data**; and sizes of program resource items **within said resource data**" (emphasis added), as claimed by applicant.

Moreover, with respect to Claim 14 et al., the Examiner has relied on the following excerpt from the Hypponen reference to make a prior art showing of applicant's claimed technique "wherein said checksum value is rotated between each item being added into said checksum."

> "For the purposes of this example, **the signature used is a checksum derived using a suitable checksum calculation algorithm, such as the US Department of Defence Secure Hash Algorithm (SHA)** or the older CRC 32 algorithm." (Hypponen, Col. 4, lines 56-59 - emphasis added)

Applicant asserts that the excerpt from Hypponen relied upon by the Examiner teaches that "the signature used is a checksum derived using a suitable checksum calculation algorithm, such as ... SHA." However, applicant respectfully asserts that the SHA algorithm rotates intermediate values used in the calculation of the SHA checksum

which simply fails to meet a technique "wherein said checksum value is rotated **between each item** being added into said checksum" (emphasis added), as claimed by applicant.

In addition, with respect to Claim 12 et al., the Examiner has rejected the same under 35 U.S.C. 103(a) as being unpatentable over Cozza in view of Hypponen as applied to Claim 4 et al., in further view of Hodges et al. (U.S. Patent No. 6,269,456). Specifically, the Examiner has relied on the following excerpts from the Hodges reference to make a prior art showing of applicant's claimed technique "wherein said fingerprint data includes timestamp data indicative of a time of compilation of said known computer program."

> "Generally speaking, a recent trend is for manufacturers of antivirus applications to update their virus signature files VIRUS_SIGNATURES.DAT as new viruses are discovered and as cures for these viruses are developed, and to make these updated signature files available to users on a periodic basis (e.g. monthly, quarterly, etc.). For example, an antivirus program manufacturer may post the update file VIRUS_SIGNATURES.DAT on a bulletin board system, on an FTP (File Transfer Protocol) site, or on a World Wide Web site for downloading by users." (Hodges, Col. 2, paragraph 6 - emphasis added)

> "These and other objects are achieved by a method and system for updating local client computers with antivirus software updates from a central antivirus server, the local client computers and the central antivirus server being coupled by a packet-switched network, wherein the antivirus software updates are transferred from the central antivirus server to a given local client computer using a push technology method. The central antivirus server comprises a first database containing information related to the latest antivirus software updates contained on each local client computer, and uses push technology to transmit updated antivirus files if the local client computer's antivirus files are out of date." (Hodges, Col. 4, paragraph 6 - emphasis added)

Applicant asserts that the excerpts from Hodges relied upon by the Examiner merely teach that "manufacturers of antivirus applications ... update their virus signature files VIRUS_SIGNATURES.DAT as new viruses are discovered and as cures for these viruses are developed." In addition, Hodges teaches using "push technology to transmit updated antivirus files if the local client computer's antivirus files are out of date." However, the disclosure of updating antivirus signature files simply fails to even suggest

a technique "wherein said fingerprint data includes timestamp data indicative of a time of compilation of said known computer program" (emphasis added), as claimed by applicant. There simply is no mention in the excerpts from Hodges anything regarding the use of "time of compilation of said known computer program" in the fingerprint data, as claimed by applicant.

Thus, a notice of allowance or specific prior art showing of each of the foregoing claim elements, in combination with the remaining claimed features, is respectfully requested.

Still yet, applicant brings to the Examiner's attention the subject matter of new Claims 97-98 below, which are added for full consideration:

"wherein said fingerprint data includes a checksum value calculated in dependence upon:

a number of program resource items specified beneath each node within hierarchically arranged resource data;

string names associated with program resource items within said resource data; and

sizes of program resource items within said resource data" (see Claim 97); and

"wherein said checksum value is rotated 1 bit to the left" (see Claim 98).

Again, applicant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art references, when combined, fail to teach or suggest all of the claim limitations, as noted above. To this end, a notice of allowance or specific prior art showing of each of the foregoing claim elements, in combination with the remaining claimed features, is respectfully requested.

Thus, all of the independent claims are deemed allowable. Moreover, the remaining dependent claims are further deemed allowable, in view of their dependence on such independent claims.

In the event a telephone conversation would expedite the prosecution of this application, the Examiner may reach the undersigned at (408) 505-5100. The Commissioner is authorized to charge any additional fees or credit any overpayment to Deposit Account No. 50-1351 (Order No. NAI1P467).

Respectfully submitted,
Zilka-Kotab, PC.

Kevin J. Zilka
Registration No. 41,429

P.O. Box 721120
San Jose, CA 95172-1120
408-505-5100